IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH DOMAINS HADESHOP.ST AND HADESHOP.IO THAT IS STORED AT PREMISES CONTROLLED BY SHOCK HOSTING	Case No. 2:22-mj-165 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Seth Erlinger, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Shock Hosting LLC, an internet services provider (ISP) registered at 200 Centennial Avenue, Suite 200, Piscataway, New Jersey 08854. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Shock Hosting LLC to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since September 2017. I am currently assigned to the Cincinnati Field Office, Cyber Crime Squad, which is responsible for investigating computer and high-technology crimes, and I am trained and authorized to investigate the offenses alleged herein. Since my assignment to the Cyber Crime

Squad, I have received both formal and informal training from the FBI regarding cyber investigations.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1030(a) (computer intrusion) have been committed by unknown individuals operating the online marketplace known variously as Hades Shop, Hadeshop.st, and Hadeshop.io (hereinafter, "Hades Shop"). There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. In September 2021, the FBI identified the online marketplace using the name Hades Shop. A review of the site revealed it advertised a variety of items for sale, including credentials in these categories:

a. Remote Desktop Protocol (RDP);

b. Simple Mail Transfer Protocol (SMTP);

c. Control Panel (cPanel);

d. Shell; and

e. Office 365 (O365) webmail.

7. Law enforcement determined the Hades Shop site was hosted by Shock Hosting LLC at IP address 104.36.229.135.

8. On or about September 16, 2021, the FBI served Shock Hosting with a preservation letter for data related to Hades Shop and IP address 104.36.229.135.

9. Open-source "WhoIs" information[1] for Hadeshop.io revealed it was created on or about May 25, 2020, while Hadeshop.st was created on or about December 23, 2020. Hades Shop also has two alternate domains, Hadeshop.cc and Hadeshop.xyz, both of which were created on June 16, 2020.

10. On February 22, 2022, the FBI made undercover purchases with cryptocurrency[2] of cPanel credentials, Shell access, and O365 credentials from Hades Shop.

11. Two of the purchases provided access to interactive PHP shells.[3] The shells were branded with the "AnonymousFox" logo, and included menus for "Infect," "HackerTools," "SpammerTools," and "BruteForce," among others.

12. Based on open-source information, AnonymousFox is both the name of a group that shares or sells website exploitation and hacking tools, as well as the name used for the hacking tool suite used in compromised website environments. The AnonymousFox hacking tool suite

---

[1] WhoIs allows anyone to query a database of people and other Internet entities, such as domains, network, and hosts. The data typically includes company/individual name, address, phone number, and email.

[2] Cryptocurrency is any form of currency that exists digitally or virtually and uses cryptography to secure transactions.

[3] An interactive PHP shell can be used for the administration and maintenance of a website, and provides direct access to a server on which a site is hosted. The shell provides an interface where a user can type PHP code and execute it directly on the server.

leverages different tools and techniques to identify vulnerable websites, exploit vulnerable access points, and spread across environments. AnonymousFox exploits vulnerable plugins and extensions in use on many content management systems, including WordPress, Joomla, and Opencart, among others.[4]

13. Based on my training and experience, the exploitation of vulnerable website plugins or browser extensions can provide an actor unauthorized access to a server hosting a website or a computer, in violation of 18 U.S.C. §§ 1030(a).

14. The O365 webmail account was for a user under the go.pasadena.edu domain, used by the Pasadena City College in California.

15. On March 1, 2022, a Detective from the Pasadena City College confirmed that the email account from which the FBI purchased credentials from Hades Shop was a legitimate account at Pasadena City College.

16. On or about February 25, 2022, representatives of Shock Hosting LLC confirmed there had been no changes to the Shock Hosting client identified as a result of the FBI's September 16, 2021 preservation letter.

17. Based on the above, there is probable cause to believe the Hades Shop marketplace is selling access to compromised servers and online accounts, in violation of 18 U.S.C. §§ 1030(a) (computer intrusion).

BACKGROUND CONCERNING ISPs

18. In my training and experience, I have learned that Shock Hosting LLC provides a variety of on-line services, including dedicated servers, to the public. Subscribers obtain an

[4] Sucuri Security, https://sucuri.net/guides/anonymousfox-hack-guide/

account by registering with Shock Hosting LLC. During the registration process, Shock Hosting LLC asks subscribers to provide basic personal information and payment information. Therefore, the computers of Shock Hosting LLC are likely to contain stored electronic communications and information concerning subscribers and their use of Shock Hosting LLC services, such as account access information, data transfer information, and stored data. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

19. In my training and experience, ISPs generally ask their subscribers to provide certain personal identifying information when registering for an internet services. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

20. In my training and experience, ISPs typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.* session) times and durations, the types of service used, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, ISPs often have records of the Internet Protocol address (IP address) used to register the

account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

21. In my training and experience, in some cases, internet services account users will communicate directly with an ISP about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. ISPs typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

22. As explained herein, information stored in connection with an internet services subscriber account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an internet services subscriber account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, network traffic logs, server event logs, and server control panel logs (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the ISP can show how and when the account was accessed or used. For example, as described below, ISPs typically log the IP addresses from which users access the account, along with the time and date of that access. By

determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time. Last, stored electronic data may provide relevant insight into the account owner's state of mind as it relates to the offense under investigation. For example, information in the account may indicate the owner's motive and intent to commit a crime (*i.e.* communications relating to the crime), or consciousness of guilt (*i.e.* deleting communications or logs in an effort to conceal them from law enforcement).

CONCLUSION

23. Based on the foregoing, there is probable cause to believe the Hades Shop marketplace is selling access to compromised servers and online accounts, in violation of 18 U.S.C. §§ 1030(a) (computer intrusion) and I respectfully request that the Court issue the proposed search warrant.

REQUEST FOR SEALING

24. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

Seth Erlinger
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on March 11, 2022

HONORABLE CHELSEY M. VASCURA
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Hadeshop.st and Hadeshop.io that is stored at premises owned, maintained, controlled, or operated by Shock Hosting LLC, a company registered at 200 Centennial Avenue, Suite 200, Piscataway, New Jersey 08854.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Shock Hosting LLC (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to the Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on September 16, 2021, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information pertaining to that account or identifier, including all files, databases, and database records stored by the Provider in relation to that account or identifier;

b. All information in the possession of the Provider that might identify the subscribers related to those accounts or identifiers, including names, addresses, telephone numbers and other identifiers, e-mail addresses, business information, the length of service (including start date), means and source of payment for services (including any credit card or bank account number), and information about any domain name registration;

c. All records pertaining to the types of service used by the user, including any other accounts or identifiers;

d. The contents of and all records pertaining to all electronic communications between the Provider and any person regarding the account or identifier, including contacts with support services and records of actions taken from on or about May 25, 2020 to the present;

e. All stored data, virtual machine backups, records or other information stored by an individual using the account.

The Provider is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. §§ 1030(a) (computer intrusion), those violations involving Hadeshop.st and/or Hadeshop.io and occurring after May 25, 2020, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

1. Evidence relating to the procurement, use, sale, and/or distribution of personally identifiable information;
2. Evidence relating to the procurement, use, sale, and/or distribution of methods to access a computer, such as remote desktop protocol credentials, control panel credentials, PHP shell locations, email credentials, and lists of emails for phishing;
3. Evidence relating to computer intrusion, and/or communications with individuals or entities related to computer intrusion;
4. Evidence relating to cryptocurrency transactions;
5. Evidence indicating how and when the account identifier was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
6. Evidence indicating the account identifier owner's (the "Subscriber") state of mind as it relates to the crime under investigation;
7. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);
8. files, databases, and database records stored by the Provider on behalf of the Subscriber or user operating the website, including:
    a. programming code used to serve or process requests made via web browsers;

b. HTML, CSS, JavaScript, image files, or other files;

c. HTTP request and error logs;

d. SSH, FTP, or Telnet logs showing connections related to the website, and any other transactional information, including records of session times and durations, log files, dates and times of connecting, methods of connecting, and ports;

e. MySQL, PostgreSQL, or other databases related to the website;

f. email accounts and the contents thereof, associated with the account;

9. Subscriber information related to the accounts established to host the site enumerated in Attachment A, to include:

a. Names, physical addresses, telephone numbers and other identifiers, email addresses, and business information;

b. Length of service (including start date), types of service used, means and source of payment for services (including any credit card or back account number), and billing and payment information;

c. If a domain name was registered on behalf of the subscriber, the date that the domain was registered, the domain name, the registrant information, administrative contact information, the technical contact information and billing contact used to register the domain and the method of payment tendered to secure and register the Internet domain name

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted

by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Shock Hosting LLC, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Shock Hosting LLC, and they were made by Shock Hosting LLC as a regular practice; and

b. such records were generated by Shock Hosting LLC's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Shock Hosting LLC in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Shock Hosting LLC, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature